UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1709 Boyden Street, Greensboro, NC 27403 (described in Attachment A hereto)

Case No. 1:21MJ429-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

1709 Boyden Street, Greensboro, NC 27403 (described in Attachment A hereto)

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence related to threats, including computers, electronic devices, firearms, ammunition listed in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875(c)	Interstate Communication of Threat to Injure

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Norman G. Kuylen
Applicant's signature

Norman G. Kuylen, Special Agent, FBI
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 11/17/2021 5:01p.m.

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF

AN APPLICATION FOR A SEACH WARRANT

I, Norman G. Kuylen, being first duly sworn on oath, on information and belief state:

INTRODUCTION, BACKGROUND, TRAINING, AND EXPERIENCE

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to search 1709 Boyden Street, Greensboro, North Carolina, ("the Premises") which is described in Attachment A, for evidence of violations of 18 U.S.C. § 875(c) (interstate communication of threat to injure), which is further described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January 2003. Since November 2008, I have been assigned to the Charlotte Division/Greensboro Resident Agency, where I have been charged with investigating multiple violations of federal law, including, but not limited to, transnational drug and firearms trafficking, money laundering, threats of violence, and national security matters, defined under Title 18 of the United States Code. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, cellular telephone extractions, interviews, and debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

3. The facts in this affidavit come from my personal observations, training, experience, and/or information obtained from other law enforcement officers and/or witnesses.

This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 875(c) (interstate communication of threat to injure) have been committed by Melissa Roberts (Roberts) (DOB: XX/XX/1980) and Kevin Herriott (DOB: XX/XX/1985). There is also probable cause to believe that evidence of those violations will be found at the Premises.

PROPERTY TO BE SEARCHED/ DESCRIPTION OF THE PREMISES

5. 1709 Boyden Street, Greensboro, North Carolina, ("the Premises") is described as a one-level family home in a residential, dead-end street. The structure is made of light beige or white siding with a gray shingled roof. The numbers 1709 are arranged vertically on the left side of the front door, and the numbers are partially covered by vegetation and yard decorations. Several large, raised garden beds occupy the majority of the front yard. The driveway is located on the left-front side of the property, where a green Nissan Pathfinder with NC tag PFX-6755 was parked. Further, this warrant covers all vehicles located within the curtilage of 1709 Boyden Street, Greensboro, North Carolina.

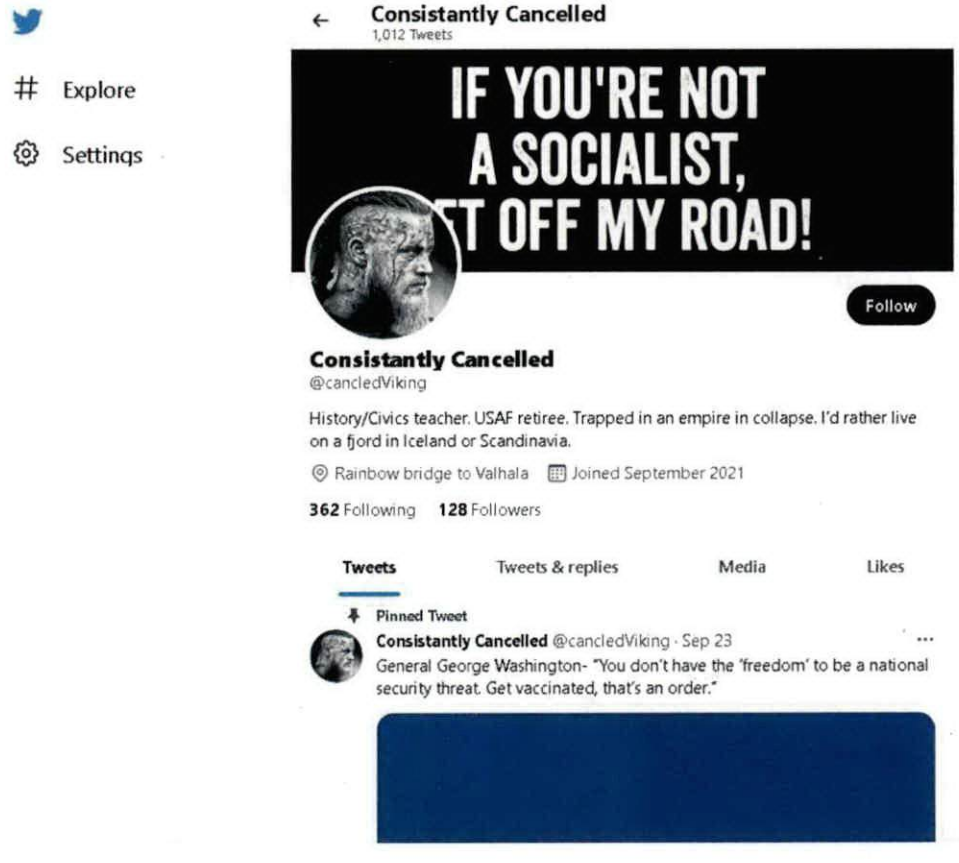
PROBABLE CAUSE

6. On August 23, 2020, there was an officer-involved shooting of an individual named Jacob Blake in Kenosha, Wisconsin. That evening, violence erupted. In the following days, rioters set fire to and damaged numerous buildings and vehicles. On August 25, 2020, Wisconsin's Governor declared a state of emergency and the National Guard was sent to Kenosha, Wisconsin. Later that evening, reports and video show numerous shots fired, involving an armed individual,

Kyle Rittenhouse, who was charged multiple counts including killing two people and injuring one person.

7. On November 1, 2021, the jury trial for Kyle Rittenhouse began in Kenosha, Wisconsin. On November 16, 2021, jury deliberations began in the trial.

8. On October 26, 2021, Twitter account username "DieuwertWubbe" alerted the Federal Bureau of Investigation (FBI) via Twitter of threatening statements posted by the Twitter account username "cancledViking." After receiving the tip, FBI observed publicly viewable postings on Twitter from Twitter account username cancledViking. The cover page of the Twitter account listed a description, "History/Civics teacher. USAF retiree. Trapped in an empire in collapse. I'd rather live on a fjord in Iceland or Scandinavia." The cover photo of the page is as follows:



9. On October 26, 2021, Twitter account username "cancledViking" posted multiple threats on Twitter against Kyle Rittenhouse, "MAGAts," and others, in general, pending the outcome of the Kyle Rittenhouse trial to include the following:

a. "The legal system can punish Kyle Rittenhouse, or I can. Bottom line, this little mf WILL NOT be another Zimmerman. Consider this my statement of intent. Fck your laws. I will not tolerate right wing violence while left wing violence is practically nonexistent."

b. "If I can't find him, some other MAGAt can take his place!"

c. "I will not tolerate him walking, even if I have to give my life to take his.".

d. "If he walks, I will be hunting him bc I'm not one of the "good ppl who stand by and do nothing.""

e. "Children don't have the right to defend themselves in public streets with a firearm. If he walks, I'll end him myself."

f. "Not my god, which is why if he walks, he will need to look over his shoulder for the rest of his fascist life."

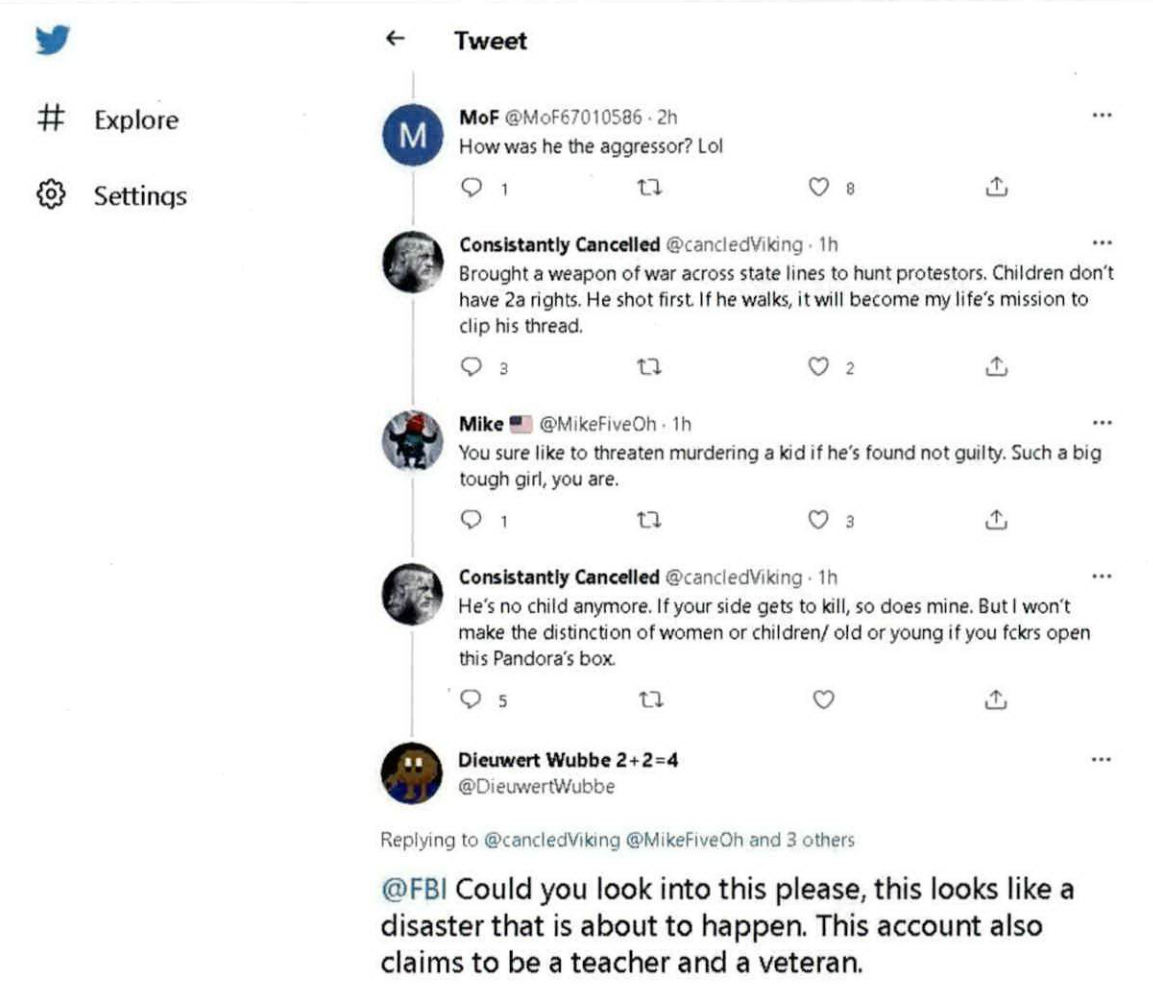
g. "If he walks, his thread will be cut!"

h. "Brought a weapon of war across state lines to hunt protestors. Children don't have 2a rights. He shot first. If he walks, it will become my life's mission to clip his thread.

i. "He's not child anymore. If your side gets to kill, so does mine. But I won't make the distinction of women or children/ old or young if you fckrs open this Pandora's box."

10. Twitter username cancledViking's post and communication threads are shown below along with the alert from DieuwertWubbe:


Consistantly Cancelled
1,014 Tweets
Follow
Consistantly Cancelled @cancledViking · 3h
Replying to @JoyAnnReid
I will not tolerate him walking, even if I have to give my life to take his.
1
Consistantly Cancelled @cancledViking · 3h
Replying to @MzSgtPepper and @LanceUSA70
If he walks, I will be hunting him bc I'm not one of the "good ppl who stand by and do nothing."
2
Consistantly Cancelled @cancledViking · 3h
Replying to @FusRohDah @CarlNyberg312 and @ajplus
Children don't have the right to defend themselves in public streets with a firearm. If he walks, I'll end him myself.
Consistantly Cancelled @cancledViking · 3h
Replying to @fredjphelps @MelnKel27 and @freekyleusa
Not my god, which is why if he walks, he will need to look over his shoulder for the rest of his fascist life.
3
Consistantly Cancelled @cancledViking · 3h
Replying to @freekyleusa
If he walks, his thread will be cut!



11. On October 26, 2021, Twitter username cancledViking posted the following threat in response to a Tweet from Twitter username "pcbrynn" regarding Texas teachers, "Not only will I not lie to my students, but if I'm fired for this, my response will be extreme violence aimed at the MAGAts responsible for my cancellation."

12. Twitter username cancledViking's post and communication thread with pcbrynn is shown below:

13. On October 21, 2021, Twitter account username "theHetal" posted on Twitter, "Do you own a gun?" On October 22, 2021, Twitter account username "cancledViking" responded, "Yes but that's bc I know the MAGAts are gonna make me use it on em."

14. Twitter username cancledViking's post and communication thread with theHetal is shown below:

15. Pursuant to a legal request, on November 6, 2021, Twitter provided subscriber information and Internet Protocol ("IP") Addresses for the Twitter account creation and dates October 22, 2021 and October 26, 2021. The account username was "cancledViking" and the account display name was "consistently Cancelled." The account was created on September 22, 2021 and had a creation IP Address of 174.249.51.184 at 18:04:13.285 UTC. The telephone number associated with the account was 336-209-6882.

16. On October 22, 2021, the following IP Addresses were used to login to the Twitter account;

a. 64.252.208.87 at 16:21:58.000 UTC;

b. 174.241.164.86 at 16:12:02.000 UTC;

c. 152.13.51.164 at 13:42:47.000 UTC;

d. 174.241.165.95 at 13:35:17.000 UTC;

17. On October 26, 2021, the following IP Addresses were used to login to the Twitter account between 11:25 UTC and 23:23 UTC:

a. 64.252.208.87 at 23:23:12.000 UTC;

b. 174.241.164.208 at 17:05:36.000 UTC;

c. 174.248.32.227 at 16:44:36.000 UTC;

d. 152.13.50.67 at 14:41:33.000 UTC;

e. 64.252.208.87 at 11:25:32.000 UTC.

18. Based on publicly available information, 64.252.208.87 was an AT&T U-Verse IP Address.

19. Based on publicly available information, 174.249.51.184, 174.241.164.86, 174.241.165.95, 174.241.164.208, and 174.248.32.227 were Verizon IP Addresses.

20. Based on publicly available information, 152.13.51.164 and 152.13.50.67 were University of North Carolina – Greensboro (UNCG) IP Addresses.

21. Based on a law enforcement database, Verizon was the carrier for telephone number 336-209-6882.

22. Pursuant to a legal request, on November 13, 2021, AT&T Global Legal Demand Center provided subscriber information associated with IP Address 64.252.208.87 on October 22, 2021 and October 26, 2021. The account number was 306121484, the account service name was Melissa Roberts, and the service address was 1709 Boyden Street, Greensboro, North Carolina ("the Premises"). The contact telephone number was 336-XXX-3067, and the contact e-mail address was melissa.roberts.336@gmail.com.

23. North Carolina Department of Transportation records reflect that Melissa Ann Roberts' (DOB: XX/XX/1980) North Carolina driver's license has 1709 Boyden Street, Greensboro, North Carolina listed as her address.

24. Based on North Carolina vehicle registrations, Melissa Roberts has a green, 2000 Nissan Pathfinder (hereinafter "Pathfinder") registered to her bearing North Carolina registration PFX-6755.

25. Based on property records, Melissa Ann Roberts and Francis Lee Roberts, Jr. co-own the residence, 1709 Boyden Street, Greensboro, North Carolina. Francis Lee Roberts, Jr. is believed to be born XX/XX/1941 and be the uncle of Melissa Roberts. Property records list the house as a single story with a basement. The main body square footage is listed as 888 square feet. The house has two bedrooms and one and a half bathrooms. North Carolina Department of Transportation records reflect that Francis Lee Roberts', Jr. North Carolina driver's license has 104 Wackena Way, Beaufort, North Carolina listed as his address. It is not believed that Francis Lee Roberts, Jr. resides at the Premises.

26. Based on the website "Coursicle" for the University of North Carolina - Greensboro, a Melissa Roberts was a professor at UNCG in the Sociology Department and taught in semesters of Fall 2020 and Spring 2021.

27. Based on the website "Rate My Professors," a Melissa Roberts was listed as a Professor in the Sociology department of UNCG who had ratings from Fall 2020.

28. On November 16, 2021, UNCG Police Department advised the FBI that Roberts was a professor at UNCG and last taught at UNCG in Spring 2021. She was enrolled as student in at UNCG in Fall 2021. On November 1, 2020, Roberts listed Shirley A. Roberts (mother), Randall W. Robert (father), and Jeff Pilkenton as emergency contacts. On November 5, 2021, Roberts updated her emergency contact as Kevin Herriott (Herriott). UNCG Police Department advised that Herriott was enrolled in History and Spanish classes at UNCG for the Fall 2021 semester. Further, previous education for Herriott included Community College Air Force (2006-2011).

29. North Carolina Department of Transportation records reflect that Kevin Herriott's (DOB: XX/XX/1985) North Carolina driver's license has 1709 Boyden Street, Greensboro, North Carolina listed as his address.

30. On November 16, 2021, law enforcement observed the green Nissan Pathfinder with NC tag PFX-6755 parked in the driveway of 1709 Boyden Street, Greensboro, North Carolina.

31. Based on my training and experience, I know that cellular telephones and other electronic devices contain information related to the device's location history, online purchases, contact lists, messaging history, photographs, internet history, call logs, appointment calendars, and application history. This information is valuable in determining where the device's user was during the commission of a crime, who they were with, what items they may have recently purchased, and other evidence of a crime.

32. Based on training and experience, I know that documents, utility bills, photos, keys and other items used to show who is in control of the "Premises" regularly provides information relating to who is actually responsible for and/or in possession of the other evidence located at a scene. I also know that these items are regularly kept in an individual's residence, on their person, or in their vehicles.

33. Based on training and experience, I know that persons who purchase firearms commonly maintain those firearms, including but not limited to handguns, pistols, revolvers, rifles, shotguns, machine guns and other weapons, as well as records or receipts pertaining to firearms and ammunition; at their place of residence and/or other locations including vehicles where they exercise dominion and control.

TECHNICAL TERMS

34. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

35. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage

media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. *Probable cause.* I submit that if a cellular phone, computer or storage medium is found on the Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system

data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect.

For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer

and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

38. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine

storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

40. Because several people may share the Premises as a residence, it is possible that the Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

41. I submit that this affidavit supports probable cause for a search warrant of "the Premises" described in Attachment A to seek the items described in Attachment B.

/S/ Norman G. Kuylen

Norman G. Kuylen

Special Agent

Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone this 17th day of November, 2021 at 5:01p.m.

The Honorable Joe L. Webster

United States Magistrate Judge

Middle District of North Carolina

Certified to be a true and
correct copy of the original.
John S. Brubaker, Clerk
U.S. District Court
Middle District of North Carolina
By: _____ Deputy Clerk
Date: November 17, 2021

ATTACHMENT A

Property to Be Searched/ Description of the Premises

1709 Boyden Street, Greensboro, North Carolina, ("the Premises") is described as a one-level family home in a residential, dead-end street. The structure is made of light beige or white siding with a gray shingled roof. The numbers 1709 are arranged vertically on the left side of the front door, and the numbers are partially covered by vegetation and yard decorations. Several large, raised garden beds occupy the majority of the front yard. The driveway is located on the left-front side of the property, where a green Nissan Pathfinder with NC tag PFX-6755 was parked. Further, this warrant covers all vehicles located within the curtilage of 1709 Boyden Street, Greensboro, North Carolina.

ATTACHMENT B

Particular Things to be Seized

All physical evidence found at the location described in Attachment A that relate to violations of 18 U.S.C. § 875(c) (interstate communication of threat to injure), to include:

1. Firearms, ammunition, firearms accessories, documents or information related to the purchase and/or sale of firearms, ammunition, firearms accessories;
2. Photographs or other documents related to firearms, ammunition, firearms accessories;
3. All indicia of occupancy, residency or ownership of the premises and things described in the warrant, including identification documents, utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents, and keys.
4. Records and information relating to communications with Internet Protocol addresses 174.249.51.184, 64.252.208.87, 174.241.164.86, 152.13.51.164, 174.241.165.95, 174.241.164.208, 174.248.32.227, and 152.13.50.67.
5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

6. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, cellular telephones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. Cellular telephones for any of the suspects;

8. Maps or other indications of planning;

9. All records, items and documents reflecting travel for the purpose of participating in the aforementioned interstate communication of threat to injure, including but not limited to gas station receipts, store receipts, credit card receipts, restaurant remaps, and records of long-distance calls reflecting travel;

10. Accounting records, specifically financial statements, bank records, ledgers, journals, check registers, and other books and records used to maintain a record of income and expenses;

11. Checking, savings, and investment account records, including signature cards, account statements, deposit receipts, withdrawal receipts, cancelled checks, money orders, cashier's checks, records of incoming and outgoing wire transfers, electronic funds transfer records, checkbooks, credit card record and receipts, including supporting documentation and schedules, and any other records of documents pertaining to the receipt, expenditure, or concealment of money;

12. Any and all of the above listed evidence stored in the form of magnetic or electronic coding on computer media or media capable of being read by a computer or with the aid of computer-related equipment, including but not limited to floppy disks, fixed hard disks, removable hard disks, tapes, laser disks, videocassettes, CD-ROM's, DVD disks, Zip disks, smart cards, memory sticks, memory calculators, personal digital assistants

(PDS's), cellular telephones, and/or other media capable of storing magnetic coding, the software to operate them and related instruction manuals;

13. All electronic devices which are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer impulses or data. These devices include computers, computer components, computer peripherals, word processing equipment, modems, monitors, printers, plotters, encryption circuit boards, optical scanners, external hard drives, and other computer related electronic devices;

14. The search procedures of the electronic data contained in computer operating software or memory devices, whether performed on site or in a laboratory, or other controlled environment, may include the following techniques:

    a. Surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

    b. "Opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

    c. "Scanning" storage areas for deliberately hidden files; or

    d. Performing key word searches through all electronic storage areas to determine whether occurrences of languages contained in such storage areas exist that are intimately related to the subject matter of the investigation.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.